U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.260
May 21, 1999

GUIDE TO PROTECTING INFORMATION TECHNOLOGY

TABLE OF CONTENTS

GUIDE TO PROTECTING INFORMATION TECHNOLOGY

1. PURPOSE

The purpose of this Guide is to provide guidance in implementing, administrating, maintaining and updating the Information System Protection Program defined within the DOT H 1350.250 series of Guides for the Department of Transportation (DOT) and its Operating Administrations.

2. SCOPE

The provisions of this document apply to all DOT employees, volunteers and contractor support personnel.

3. GOALS

The goal of this document is to improve the security of DOT Information Systems by providing those DOT employees responsible for implementing the Information System Protection Program with the guidance necessary for effective Program implementation, administration, maintenance and updating.

4. REFERENCES

All references and terms used in this document are listed and explained in DOT H 1350.2.1, *ISS References/Definitions*, dated March 3, 1999.

5. OVERVIEW OF THE DOT INFORMATION SYSTEM SECURITY PROGRAM

DOT H 1350.2 defines the overall Information System Security Program within DOT and its Operating Administrations as a hierarchy of five major elements:

a. Policy – Consists of the purpose**,** goals and scope of the DOT Information System Security (ISS) Program. This element also includes the identification of the key roles and responsibilities for the successful safeguarding of DOT information. Policy is documented within DOT H 1350.2

b. Terms - Provides a description of the references used in the establishment of the ISS Program, as well as the definition of terms commonly used throughout the program documentation. Terms are documented within DOT H 1350.2-2.

c. Planning – This element incorporates all of the planning required to establish an ISS Program. Specific topics include Information System Security Plans, Risk Assessments, Certification/Accreditation, Continuity of Operations, Incident Handling, Personnel Security, Physical/Environmental Security and Awareness/Training/Education. Planning guidance is contained within the DOT H 1350.250 series of documents.

d. Requirements - This element focuses on the implementation, administration, maintenance and updating of the ISS Program, as planned, including the specific responsibilities of the key implementers/administrators, and their interactions with each other. Guidance is contained within this document (DOT H 1350.260).

e. Training - The primary key to a successful ISS Program is the Awareness and Training of owners, managers, administrators and users of the system. Awareness and training guidance is contained within the DOT H 1350.270 series of documents.

In an overall sense, the objective of the DOT ISS Program is to define, develop, implement, administer, maintain and update, as necessary, those security controls necessary and sufficient to provide an acceptable level of security risk, at an acceptable level of cost, for each DOT Information System. Security controls may be categorized as:

1) Management Controls - Management Controls addresses security topics that can be characterized as managerial in nature. They are techniques and concerns that are normally addressed by management in an organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization. Management controls focus on the management of the computer security system and the management of risk for a system.

2) Operational Controls - Operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise – and often rely upon management activities as well as technical controls.

3) Technical Controls - Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization.

6. ROLES & RESPONSIBILITIES

In the generic case, there are three individuals with specific security concerns and responsibilities associated with each DOT Information System:

a. Information System Owner – possesses overall responsibility for a DOT Major Application or General Support System. The System Owner's security role and responsibilities lie primarily in the area of Management Controls. Detailed security guidance for System Owners may be found in Attachment A, *System Owner's Security Handbook.*

b. Information System Security Officer (ISSO) – reporting to the System Owner, possesses overall responsibility for Information System Security. The ISSO therefore must be concerned with all three types of security controls, with a special focus on Operational Controls. Detailed guidance for ISSOs may be found in Attachment B, *ISSO Handbook.*

c. Information System Administrator (ISA) – reporting to the System Owner, possesses day-to-day operational responsibility for a Major Application or General Support System. The ISA's security role and responsibilities lie primarily in the area of Technical Controls. Detailed guidance for ISAs may be found in Attachment C, *ISA Security Handbook.*

Roles and responsibilities for each of these individuals are summarized in Table 1.

In addition to the abovementioned individuals, other DOT employees and organizations play a role in protecting DOT Information Systems, such as Property Managers of Secretarial Offices or Operating Administrations, the Director of the Office of Security and Administrative Management, Acquisition and Contracting Officers, etc. Refer to DOT H 1350.2 (DIRMM) for a complete listing of the responsibilities of these individuals.

POSITION	IMPLEMENTATION	ADMINISTRATION	MAINTENANCE	UPDATE
System Owner	• Review/Approve Security Plans • Set Implementation Priorities • Provide Overall Leadership and Direction • Verify Implementation • Execute all necessary MOUs	• Analyze Patterns of Non-Compliance • Ensure Execution of Awareness & Training Programs • Monitor Effectiveness of Security Policy & Procedures	• Ensure Annual Maintenance of Remediation Plans	• Assess Impacts of Proposed Updates • Approve Update Plans & Schedules
ISSO	• Lead the Establishment of the ISS Program • Ensure the Integration of Mgmt, Operational & Technical Controls • Prepare Applicable MOUs with System Owners	• Ensure that New Systems meet Security Requirements • Ensue that Personnel are Cleared and have Appropriate Access • Schedule Awareness & Training Sessions • Participate in CSIRT Activities • Periodic Checks w/DOT ISSO and other Orgs regarding New Security Issues	• Perform Periodic Risk Assessments • Perform Periodic Certification of Sensitive & Classified Systems • Schedule & Perform Periodic Testing of COOP & Incident Handling	• Evaluate Need for Update based on Maintenance Activities, Policy Changes, etc. • Update Security Plan as Req'd • Lead ISS Program Update Activities
ISA	• Properly Configure HW & SW • Set Appropriate Security Features & Controls • Assist in Computer Security Incident Response Team (CSIRT) Implementation • Assist in Implementing Physical Controls • Implement Backup Procedures	• Periodically Review Security Features & Control Settings • Periodically Check w/HW & SW Vendors Regarding Security Problems, Patches, etc. • Participate in CSIRT • Monitor System Operation • Notify ISSO of Suspected misuse or misconduct • Establish, Manage and Close User Accounts • Ensure that Backups are Performed	• Participate in Periodic Certification of Sensitive & Classified Systems • Participate in COOP & Incident Handling Testing	• Install Security Patches & other Fixes as Appropriate • Assist in Preparation of COOP Updates • Periodic Update of AntiVirus SW

TABLE 1, Summary of Roles & Responsibilities

7. ISS PROGRAM IMPLEMENTATION

The DOT ISS Program Implementation process flow, culminating in Information System Accreditation and "Authority to Operate" is shown in Figure 1 below.

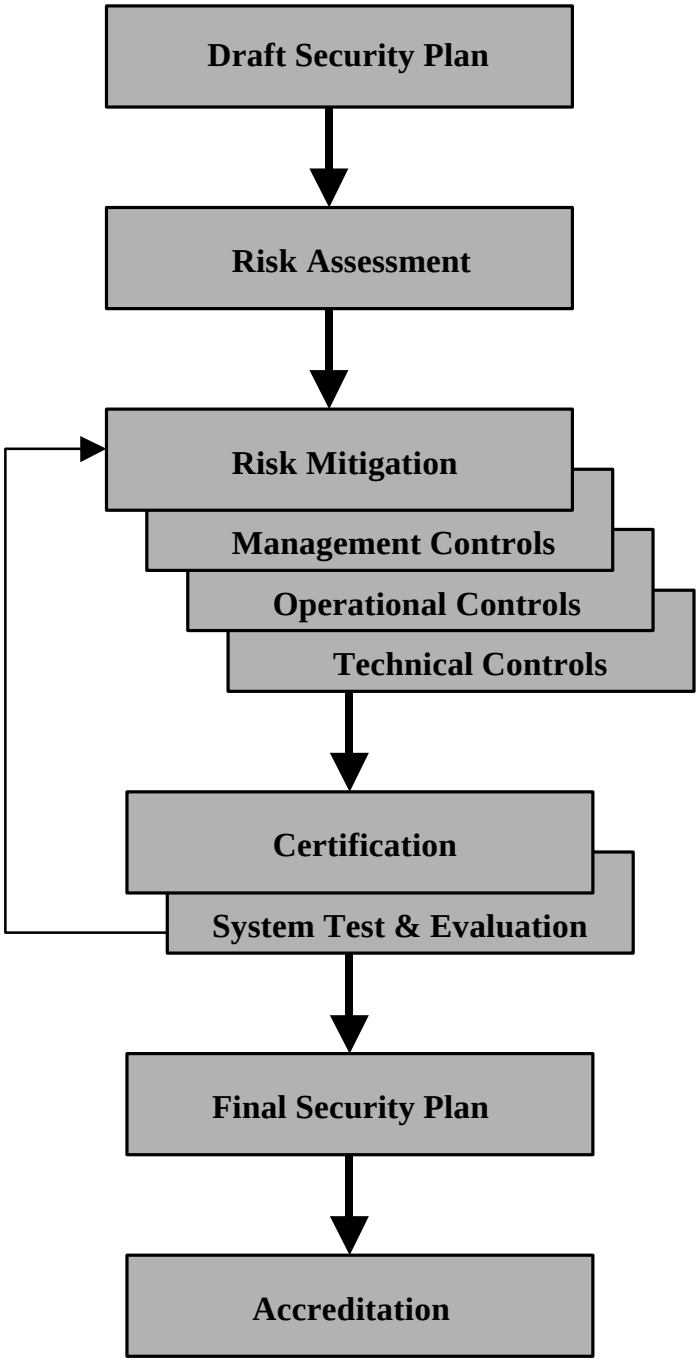

FIGURE 1, DOT ISS Implementation Process

Guidance in planning each step in the process is contained within the DOT H 1350.250 series of documents.

A. Draft Security Plan

The first step in the implementation process is the creation of a draft System Security Plan, using the form and format presented in DOT H 1350.251 *Departmental Guide to Developing an Information System Security Plan*. The Plan should provide an overview of the security requirements of the Information System, describe the controls in place or planned for meeting those requirements, and delineate responsibilities and expected behavior of all individuals who access the system. Initially, not all areas of the Plan may be definable, but as the implementation process progresses, these areas may be backfilled. The intent is that the Security Plan be a 'living document', that will always reflect the current security posture of the Information System (Major Application or General Support System) it was originally created for.

B. Risk Assessment

Risk Assessment is a formalized process for identifying, analyzing and interpreting the risks associated with an Information System, as defined in DOT H 1350.252 *Departmental Guide to Risk Assessments*. Its purpose is to provide management with a clear picture of the current overall security posture of the target System, and provide the data necessary for them to make informed decisions regarding the need for additional Risk Mitigation.

C. Risk Mitigation

Categories of Risk Mitigation include Management, Operational and Technical Controls. The specific controls required within each category will depend on the results of the Risk Assessment, and the ensuing management decisions regarding which risks require mitigation, and which risks can reasonably be assumed.

D. System Certification

System Certification includes the process of reviewing all existing System Security documentation and performing a System Test & Evaluation (ST&E) of all system safeguards and countermeasures identified in the System Security Plan, followed by a Certification that all such documentation and countermeasures have been validated and proven to be effective. Should the documentation review or ST&E uncover a problem with a particular system safeguard, that problem must be attended to prior to receiving Certification. Refer to DOT H 1350.253 *Departmental Guide to Certification/Accreditation of Information Systems* for additional guidance on System Certification.

E. Final Security Plan

With System Certification achieved, the System Security Plan is then updated to reflect all in-place Management, Operational and Technical Controls, as well as the responsibilities and expected behavior of all individuals who access the System. The Final Plan becomes the key document comprising the Accreditation Package reviewed by the Designated Accreditation Authority.

F. System Accreditation

The final step in the implementation process is to obtain System Accreditation from the DOT Designated Accreditation Authority (DAA). In order for the DAA to evaluate the overall security posture of the System, he/she will review a prepared Accreditation Package, containing all information and documents necessary to make a sound, well-informed determination of the General Support System or Major Application to operate, while still ensuring the confidentiality, availability and integrity of the information processed, stored or disseminated therein. Refer to DOT H 1350.253 *Departmental Guide to*

Certification/Accreditation of Information Systems for specific guidance in preparing an Accreditation Package. Once the DAA has reviewed the Package, and signed an Accreditation Statement, the Information System is given an 'Authority To Operate'.

8. ISS PROGRAM ADMINISTRATION

Emplacing an Information System Security Program for a DOT Major Application or a General Support System is necessary, but not sufficient to ensure continuing protection of that System. Once put in place, the Program requires continuing administration, as well as maintenance and updates. The lead individual for ISS Program Administration is the ISSO, supported by the ISA as appropriate, both reporting to the System Owner. Note that if an ISSO is assigned more than one Major Application or General Support System, he/she may be required to interface with multiple ISAs in administering the organization's ISS Program.

ISS Program Administration encompasses both the "everyday" planned tasks associated with Information Protection (e.g., opening and closing user accounts, scheduling a security training course, handling the disposal of sensitive waste) and the unplanned security incidents and emergencies which require immediate attention (e.g., the activation of the CSIRT, or the COOP). Normal administrative duties include:

- Personnel – Personnel security administration includes the control of access to equipment and data, as well as the hiring and termination of employees. Of particular significance in this regard is the issue of employee termination. Termination of an employee, whether friendly or unfriendly, is a traumatic experience for most organizations. Friendly termination refers to the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Unfriendly termination, on the other hand, involves the removal of an employee under involuntary or adverse conditions. Especially in the latter case, the potential for damage to an organization's information infrastructure can be extremely high. Processes for handling terminations are discussed in DOT H 1350.256 *Departmental Guide to Personnel Security Planning.*

- Equipment – Equipment security administration, includes configuration management, physical access control and equipment inventory tracking. It also includes the protection of System elements against damage and destruction caused by disasters such as a major fire or loss of supporting utilities (refer to DOT H 1350.257 *Departmental Guide to Physical/Environmental Security Planning).*

- Data – Data security administration includes the storage and control of access to sensitive data, the proper identification/marking of data, processes for data transportation (both within and outside of the organization), scheduled backup of data and its subsequent storage and retrieval, and the proper disposal of data (including data on magnetic media). Since many of these areas are the responsibility of the System user, they are discussed in detail in DOT H 1350.272 *Guide to Information Protection for Users*.

For a detailed description of ISS Program Administration activities, in terms of System Owner, ISSO and ISA duties and responsibilities, refer to the appropriate Sections within Attachment A (System Owner's Security Handbook), Attachment B (ISSO Handbook) and Attachment C (ISA's Security Handbook) to this Guide.

9. ISS PROGRAM MAINTENANCE AND UPDATE

In order to ensure that the level of Information Protection remains as high as when the ISS Program was first initiated, System Owners, ISSOs and ISAs must institute an aggressive set of proactive maintenance and update procedures. Focusing solely on reacting to security issues, incidents and problems, while absolutely necessary, is not sufficient by itself to cope with the

ever-changing environment under which DOT Information Systems must operate. Proactive measures emphasize:

- Periodic Test & Evaluation of Existing Security Practices and Procedures – Specific security practices and procedures (e.g., COOP, Incident Handling, Security Awareness Techniques) require periodic test & evaluation, not only to maintain consistent levels of training, but also to assess continuing applicability and effectiveness, in light of planned and unplanned changes to the overall system environment.

- Continual Evaluation of Announced Changes, Updates and Enhancements to Existing Security Products – Equipment manufacturers are constantly seeking ways to improve their security products, and to correct problems that may have been uncovered during actual product use. ISAs and ISSOs must maintain an awareness of both existing and planned changes, assess the impact of these changes on current System Technical and/or Operational Controls, and provides System Owners with recommendations regarding product updates.

- Evaluation of 'Lessons Learned' – The ability of existing System Security Controls to adequately handle actual security incidents, issues and problems requires continual evaluation by System Owners, ISSOs and ISAs. It is important to be able to identify what works well, and what doesn't work within the existing ISS Program, and be able to learn from both. The ISS program should include the ability to archive lessons learned from day-to-day ISS Program Administration, which may then be periodically assessed by the appropriate individual or individuals. Note that assessment should be done both on a case-by-case basis, and by grouping like incidents. The latter technique helps to identify trends that might not otherwise be evident from the review of a single security incident.

- Periodic Review of New Security Technology – In addition to other proactive measures, both the ISSO and ISA should periodically review public, legal and vendor information sources regarding intruder trends, new virus strains, new attack scenarios and new tools that could improve the effectiveness of DOT security controls.

In addition to proactive maintenance/update practices, there are specific "trigger" events that require the initiation of maintenance and/or update actions. These include:

- Planned Changes to Information System Architecture and/or Operation – Whenever a significant change is contemplated for a Major Application or General Support System, --- where significant is defined as potentially impacting the effectiveness of existing Security Controls, --- the ISSO must initiate a new Risk Assessment. Should the results of the Risk Assessment indicate the need for changes to the existing ISS Program, the recommendations should be presented to senior management for action.

- Identified Security Shortfall – A major security incident, or an emergency (man-made or natural) requiring the initiation of the COOP will often uncover problems with the existing security posture of the affected Information System. If the severity or impact of the incident or emergency was severe, a new risk assessment for the Information System should be considered. In other cases, a change to policy or procedures, or the addition of a new security tool may be sufficient to mitigate the uncovered risk. In either case, the ISSO should take the lead in responding to such "trigger" events.

- Periodic Review of "Authority to Operate" – The "Authority to Operate" granted by the DAA should be reviewed at least every three years (or sooner, depending on the level of risk and the potential magnitude of harm). This review becomes, in effect, a total reaccreditation, including risk assessment, risk mitigation, and recertification processes. In such instances, the same process utilized for the original accreditation should be followed. A successful reaccreditation should result in a renewed "Authority to Operate".

ATTACHMENT A - SYSTEM OWNER'S SECURITY HANDBOOK

ATTACHMENT B - INFORMATION SYSTEMS SECURITY OFFICER HANDBOOK

1. INTRODUCTION

1.1 Purpose

This Attachment provides specific guidance to Department of Transportation (DOT) Information System Security Officers (ISSOs) for implementing and maintaining the security of their assigned Information System(s).

1.2 References

All references and terms used in this document are listed and explained in DOT H 1350.2.1, *ISS References/Definitions*, dated March 3, 1999.

2. OPERATIONAL ENVIRONMENT

In order to implement an effective Information System Protection Program, the ISSO must have a clear understanding of that System's operating environment, to include the overall mission, floor layout, hardware configuration, software, type of information processed, user organizations and security clearances, operating mode, interconnections to other systems/networks of users, their security personnel, and associated responsibilities. The ISSO should refer to the appropriate Information Systems Security Plan for detailed data regarding the System's operating environment, to include the System's mission, floor layout, software, information types, user organizations, operating mode and interconnections to other systems and/or networks.

3. ISSO AREAS OF RESPONSIBILITY

This Section defines the ISSO's areas of responsibility, as regards the security of assigned information systems, in accordance with DOT H 1350.2 and NCSC-TG-027 (the Turquoise Book). The ISSO should remember, however, that the responsibility for information security rests with all users of DOT information systems, and not just with its security personnel. Refer to DOT H 1350.2 (DIRMM), Section 7.i for a specific listing of ISSO responsibilities.

3.1 Security Regulations and Policies

The ISSO shall be aware of all directives, regulations, policies, and guidelines that address the protection of classified information, as well as sensitive unclassified information. The ISSO shall also participate in the development or revision of System-specific security safeguards and local operating procedures that are based on the above regulations. The overall system security document is the Information System Security Plan, which contains all necessary security procedures, instructions, operating plans, and guidance.

The ISSO shall also provide input to other security documents, for example, security incident reports, equipment/software inventories, operating instructions, technical vulnerability reports, and contingency plans.

3.3 Mission Needs

The ISSO shall understand the goals and objectives of his/her organization, and the security resources required to support the accomplishment of these goals. Requirements may be identified by analyzing current capabilities, available resources, facilities, funding, and technology base, and by determining whether they are sufficient to fulfill the organization's mission. If not, mission needs should be evaluated and prioritized and a remediation plan developed to address these needs. Because security requirements should be included in the mission needs and current assets assessment, it is important for the ISSO to become involved in the mission definition process.

3.3 Physical Security Requirements

In general, physical security addresses the security of the facility that houses the components of the assigned Information System(s), the personnel that operate it, and the information processed thereon. Physical security also addresses contingency plans, and the maintenance and destruction of storage media and equipment. These physical safeguards must meet the minimum requirements established for the highest classification of data stored at the site. The ISSO, in coordination with DOT security personnel, is responsible for ensuring that all necessary physical safeguards are in place.

3.4 Continuity of Operations Plans

A Continuity of Operations Plan (COOP) documents emergency response, backup operations, and post-disaster recovery procedures. The ISSO provides technical contributions concerning the overall security plans, to ensure the availability of critical resources and to facilitate system availability in an emergency situation. It is also important that all responsibilities under the plan are adequately documented, communicated, and tested at a minimum, twice per annum. Specific ISSO responsibilities during an emergency in which the COOP has been invoked are detailed within that document.

3.5 Declassification And Downgrading Of Data And Equipment

Declassification is a procedure and an administrative action to remove the security classification of the subject media. Downgrading is a procedure and an administrative action to lower the security classification of the subject media. The procedural aspect of declassification is the actual purging of the media and removal of any labels denoting classification, possibly replacing them with labels denoting that the storage media is unclassified. The procedural aspect of downgrading is the actual purging of the media and removal of any labels denoting the previous classification, replacing them with labels denoting the new classification. The administrative aspect is realized through the submission to the appropriate authority of a decision memorandum to declassify or downgrade the storage media.

Even if the assigned Information System(s) carries only SBU data, the ISSO should nonetheless be familiar with declassification and downgrading procedures. Should it ever become necessary to handle classified data, the ISSO must ensure that:

- Purging, declassification, and downgrading procedures are developed and implemented.
- Procedures are followed for purging, declassifying, downgrading, and destroying storage media.
- Procedures are followed for marking, handling, and disposing of the computer, its Peripherals, and removable/non-removable storage media.
- Any special software needed to overwrite the site-unique storage media is developed or acquired.
- Any special hardware, such as degaussers, is available.

3.6 Administrative Security Procedures

Administrative security includes the preparation, distribution, and maintenance of plans, instructions, guidelines, and operating procedures regarding security of information systems.

It is the responsibility of the ISSO to assist in the development of system administrative procedures, if required, and to conduct periodic reviews to ensure compliance.

3.6.1 Personnel Security

One component of administrative security is personnel security. In general, it is the ISSO's responsibility to:

- Ensure that all personnel and, when required, specified maintenance personnel who install, operate, maintain, or use the system, hold the proper security clearances and access authorizations.
- Ensure that all Information System users, including maintenance personnel, are educated as regards applicable security requirements and responsibilities.
- Maintain a record of valid security clearances, physical access authorizations, and System access authorizations for personnel using the System.
- Ensure that maintenance contractors who work on the system are supervised by an authorized, knowledgeable person.

The ISSO is responsible for performing the following tasks whenever any System user's access is terminated. Prompt action is required, --- particularly if the termination or knowledge of the pending termination might provoke a user to retaliate.

The ISSO performs the following in support of this task:

- Removes the user from all access lists, both manual and automated.
- Ensures that the ISA has assigned the user's files to a supervisor, eliminating the access by the user but allowing the supervisor to maintain availability.
- Ensures that the ISA has removed the individual's ID and password from all systems.
- Ensures that the individual has turned in all keys, tokens, or cards that allow access to the System.
- Ensures that the combinations that the individual possessed for any combination locks associated with the System and its physical space are changed.

3.6.2 Security Incident Handling

A security incident occurs whenever DOT information is compromised, when there is a risk of compromise of such information, when recurring or successful attempts to obtain unauthorized access to the System is detected, or where misuse of the System is suspected.

The ISSO creates a reporting mechanism, as part of the security incident reporting procedure, for System users to keep them informed of security-relevant activity that they may observe on the System. This reporting mechanism shall not use the System itself to report security-relevant activity about the System.

The mechanism, at a minimum, includes the following:

- Description of incident.
- Identification of the individual reporting the security incident.
- Identification of the loss, potential loss, access attempt, or misuse.
- Identification of the perpetrator (if possible).
- Notification of appropriate security and management personnel and civil authorities, if required.
- Reestablishment of protection, if needed.
- Restart of operations, if the system had been taken down to facilitate the investigation.

The ISSO performs the following in support of this task:

- Prepares procedures for monitoring and reacting to system security warning messages and reports.
- Develops, reviews, revises, and submits for approval to the DAA and System Owner procedures for reporting, investigating, and resolving security incidents.
- Immediately reports security incidents through the appropriate security and management channels. The ISSO submits an analysis of the security incident to the appropriate CSIRT authority for corrective and disciplinary actions.
- Performs an initial evaluation of security problems, and, if necessary, temporarily denies access to affected systems. The ISSO ensures that the Information System Administrator (ISA) evaluates, reports, and documents System security problems and vulnerabilities.
- Partially or completely suspends operations if any incident is detected that affects security of operations. This would include any system failure. (Note: this may be unrealistic if the system performs a critical operational mission. Alternative procedures may be required in this situation. The DAA must weigh the risk of a security incident against the potential damage in shutting down the System.)
- Ensures that all cases of actual or suspected compromise of classified or SBU passwords are investigated.
- Ensures that occurrences within the System that may affect the integrity and security of the data being processed are investigated. If the system malfunctions, it is important to account for the data.
- Assists the investigating officials in analyzing actual or suspected compromises of classified or SBU information, if applicable.

3.7 Security Awareness and Training

Because personnel are an integral part of the security protection surrounding the assigned Information System(s), they must understand the vulnerabilities, threats, and risks inherent with System usage. Therefore, information system security shall be included in briefings given to all new personnel. To reinforce this initial training and to introduce new concepts,

periodic training and security awareness programs should be conducted. The ISSO shall continue training to keep current in security products and procedures. The ISSO is responsible for ensuring that:

- All personnel (including management) have computer security awareness training and have read applicable sections of the Information System Security Plan and DOT H 1350.272 *Guide to Information Protection for Users*. This includes training in security procedures and the use of security products.

- All users are educated regarding password management (e.g., generating unique passwords, keeping passwords adequately protected, not sharing passwords, and changing passwords on a regular basis).

- Users understand the importance of monitoring their successful and unsuccessful logins, if possible. If these do not correspond to the user's actual usage, the user should know the proper procedures for reporting the discrepancy.

Note that new personnel could include contractors newly assigned to work at a DOT facility. Such individuals should become familiar with DOT H 1350.273 *Guide to Information Protection for Contractors*.

The ISSO can keep users informed about security in many different ways. Some approaches include:

- Periodically display messages when the user logs on to the System.

- Develop and distribute security awareness posters to foster interest.

- Disseminate new security information about the System and issue reminder notices about protection procedures.

- Issue memos or e-mail to notify users of changes.

- Provide "hands-on" demonstrations of System security features and procedures.

Security awareness and training is one of the most important features that an ISSO can implement. When security is kept prevalent in an individual’s mind through regular awareness and training, those individuals are more likely to follow the appropriate standards and guidelines.

3.8 Security Configuration Management

Configuration management controls changes to system software, hardware, and documentation throughout the life of the System. This includes the design, development, testing, distribution, and operation of modifications and enhancements to the existing System. The ISSO or other designated individual aware of the security issues shall be included in the configuration management process to ensure that implemented changes do not compromise security. It is particularly important for the ISSO to review and monitor proposed changes to the System as defined in the security architecture. Appropriate tests should be conducted to show that the System functions properly after changes are made to it. Configuration management tasks that are the responsibility of the ISSO are as follows:

- Maintain an inventory of security-relevant hardware and security-relevant software and their locations.

- Maintain documentation detailing the System hardware and software configuration and all security features that protect it.

- Evaluate the effect on security of proposed centrally developed and distributed and site-unique modifications to software and applications. Submit comments to appropriate personnel.

- Identify and analyze System malfunctions. Prepare security incident reports.

- Assist in the development of System development notifications and System change proposals.

- Monitor DAA-approved site procedures for controlling changes to the current System.

- Ensure that any System connectivity is in response to a valid operational requirement.

- Ensure that continuing tests of the site security features are performed, and maintain documentation of the results.

- Coordinate System security changes with the System Owner and ISA. Review all site configuration changes and System component changes or modifications, to ensure that Systemsecurity is not compromised.

- Review physical inventory reports of security-relevant System equipment.

The ISSO ensures that the design and development of new System equipment, or the maintenance or replacement of existing equipment includes security features that will support certification and accreditation or re-accreditation. In support of this effort, informal reviews with the System Owner and/or ISA can help identify potential problems, thus enabling potential security risks to be identified early. Before installing any new system release, the ISSO shall complete sufficient testing to verify that the system meets the documented and approved security specifications and does not violate existing security policy. The ISSO shall, at a minimum, observe the testing of new releases. Specific ISSO tasks include:

- Ensure that all security-relevant development and planning activities are reviewed and approved.

- Participate in the acquisition planning process for proposed acquisitions to ensure that DOT security policy has been considered. This applies to both the acquisition of new systems or the upgrade of existing systems.

- Ensure that security features are in place (by testing) to prevent applications programs from bypassing security features or from accessing sensitive areas of the system.

- Develop procedures to prevent the installation of software from unauthorized or questionable sources.

- Ensure that System support personnel know how to install and maintain security features.

3.9 Access Control

In this Section, access is considered from three different perspectives: physical access to the Information System facility (facility access), logical access to the System (identification and

authentication), and logical access to the System's data files and other objects (data access). Each of these perspectives is discussed separately in the following paragraphs.

3.9.1 Facility Access

Procedures shall be developed for controlling access to the System Computer Room and the System's resources. In accordance with applicable security policy, System access shall be denied to any user, customer, or visitor who has not been granted specific authorization. General guidance for the ISSO includes:

- Establish procedures to ensure that only personnel who have a need-to-know have access to classified or sensitive but unclassified information.
- Establish procedures to ensure that only personnel who have the proper clearances and formal access approval are allowed physical access to the System Computer Room. All individuals who have routine access to the Computer Room should be properly cleared and have a valid operational requirement for access.
- Deny access to any user, customer, or visitor who is unauthorized or suspected of violating security procedures.
- Ensure all visitors are signed-in and escorted, if necessary. Visitors shall be under visual observation by an authorized person.
- Keep records of maintenance performed in the System Computer Room.
- Establish and implement procedures to control System equipment coming into and going out of the Computer Room and telephone closets.
- Ensure that an authorized, knowledgeable person supervises maintenance contractors who work on the System.

3.9.2 Identification and Authentication (I&A)

The identification component of an I&A system consists of a set of unique user identifiers. Authentication involves verifying the identity of a user. If a user's identifier does not remain unique, a subsequent user may gain the access rights of a previous user on the system. General guidance to the ISSO includes:

- Ensure that the databases required to support the I&A function are accessible only by the ISSO.
- Obtain a list of all identifications (IDs) preset at the factory. Change or delete all user IDs and passwords that come with vendor software to prevent unauthorized access.
- Default passwords shall be checked and changed, as necessary, during System installation and modification, when the ISSO first assumes responsibility for the System, and after any maintenance to the System.
- Together with the ISA, develop and administer a password management system that includes the generation of System passwords and the development of procedures for addressing password loss or compromise.

- Ensure that only authorized persons execute System utility programs and routines that bypass security checks or controls.

- Maintain a System user list that contains the name, user ID, access level, and whether the user is to have operator or administrative privileges.

3.9.3 Data Access

The focus of data access procedures is to prevent disclosure of information to unauthorized individuals. General guidance for the ISSO includes:

- Ensure that the System-specific discretionary access control policy is defined and implemented. The policy should define the standards and regulations that the ISSO must implement to ensure that data is disclosed only to authorized individuals.

- Control access to all functions that can affect the security or integrity of the System. Access of this type shall be kept to the absolute minimum number of personnel.

- Ensure that any required access control software subsystems or other security subsystems are installed and operated in a manner that supports the security policy of the System.

3.10 Risk Management

Risk management identifies, measures, and minimizes the effect of uncertain events on System resources. Risk management determines the value of the data, what protection already exists, and how much more protection the System needs. The process includes risk analysis, cost benefit analysis, safeguard selection and implementation, appropriate security tests, and systems review. Risk management is an ongoing process that will reaffirm the validity of previous analysis. The ISSO supports the risk management process by performing the following tasks:

- Assist in the development of the risk management plan.

- Perform a risk assessment and analysis every three years, at a minimum, by analyzing threats to and vulnerabilities of the System Facility and vulnerabilities in relationship to the sensitivity of the information on the System. Document the results and prepare appropriate countermeasures. (This is expanded below.)

- Ensure that a contingency plan is in place for continuity of operations in an emergency situation, and that the developed plans are tested annually, at a minimum.

- Ensure that approved countermeasures are implemented.

- Periodically review the risk assessment for new threats due to a changed configuration or changes in the operational environment, and review contingency plans to ensure that they are still applicable.

- Ensure that risk analysis, security tests, TEMPEST tests, and other inspections are conducted as required. Maintain a file of working papers concerning risk analysis, security tests and other facets of the risk management program.

- Maintain a file of all site security-related waivers.

The ISSO documents and reports detected computer security technical vulnerabilities. The report includes information regarding technical solutions or administrative procedures implemented to reduce the risk. Each ISSO administers the technical vulnerability reporting program and:

- Reports identified technical vulnerabilities. As a further way of sharing information about vulnerabilities, maintains contact with other system security officers and with other users of the same type of system.
- Assumes responsibility for recommending any necessary and feasible action to reduce risks presented by the vulnerabilities.
- Develops local procedures for reporting and documenting technical vulnerabilities, and ensures that all users and operators receive training for carrying-out the procedures.
- Ensures that vulnerability information is properly classified and protected.

3.11 Audits

The ISSO has the primary responsibility to conduct security audits for operational systems as well as for systems under development. Monitoring of variances in security procedures is also important and is best controlled by the ISSO. As part of variance monitoring, the ISSO reviews any relevant audit trail data from the system. Finally, the ISSO provides senior management with reports on the effectiveness of security policy, with identification of weaknesses and recommendations for improvements.

3.11.1 Audit Trails

The audit trail provides a record of System security-related activity and allows the ISSO and the ISA to monitor activities on the System. To be an effective security tool, the audit trail should be able to monitor, for example, successful and unsuccessful access attempts, file accesses, type of transaction, and password changes. If manual audits are necessary, the ISSO shall document random checks made to verify that users are recording system usage. Audit trail files must be protected to prevent unauthorized changes or destruction.

3.11.2 Auditing Responsibilities

Appropriate audit trail data shall be reviewed by the ISSO. System audit reports can provide detailed information on network traffic and provide summary accounting information on each user ID, account, or process. The responsibilities of the ISSO include:

- Review specifications for inclusion of audit trail reduction tools that will assist in audit trail analysis.
- Select security events to be audited. Ensure that the audit trail is reviewed and have the capability to audit every access to controlled system resources (e.g., very sensitive files).
- Archive audit data.
- Develop and implement audit and review procedures to ensure that all System functions are implemented in accordance with applicable policies and programs.

Existing policies and programs usually establish the minimum amount of material that shall be audited.

- Conduct audits and maintain documentation on the results.
- Supervise review of security audit parameters. Develop, review, revise, submit for approval, and implement procedures for monitoring and reacting to security warning messages and reports.
- Conduct random checks to verify compliance with the security procedures and requirements of the site.
- Gather information from audit trails to create profiles of system users. Observe user patterns such as the terminal usually used, files accessed, normal hours of access, and permissions usually requested, to determine which actions are unusual and should be investigated.
- Review user access reports generated by the audit trail, in compliance with policies and practices.

In addition, the ISSO shall review audit trail reports for anomalies:

- Look for multiple unsuccessful logon attempts. This could be an indication of an inexperienced user, a user who has recently changed passwords and forgotten the new one, or an attempted intrusion.
- Look for an attempt by a user, who is already logged in, to log in again to the same system from a second computer. This could be caused by an inadvertent failure to log out, an intentional logon to both computers, or could be an attempted intrusion.
- Be alert to individuals logging in after normal hours. This may mean the user has a deadline to meet and is working overtime, or that an intruder is attempting access.
- Look for high numbers of unsuccessful file accesses. This could be prompted by the user’s failure to remember file names, or by an attempted intrusion.
- Look for unexplained changes in system activity.
- Look for covert channel activity.

3.12 Certification and Accreditation

System certification is the technical evaluation of the System's security features, including non-System security features (e.g., administrative procedures and physical safeguards), against a specified set of security requirements. The objective is to determine how well the System design and implementation meet this pre-defined set of security requirements. Certification is performed as part of the accreditation process. System accreditation is the formal management decision made by the DAA to implement a System in a specific operational environment at an acceptable level of risk. The certification package specifies the following in support of accreditation:

- Security mode.
- Set of administrative, environmental, and technical security safeguards.

- Operational environment.
- Interconnections to other Major Applications or General Support Systems.
- Vulnerabilities as well as procedural and physical safeguards.

The ISSO is frequently responsible for the following list of tasks in preparation for the accreditation of a System:

- Assist in preparing the accreditation material required by the DAA.
- Assist in the evaluation of the accreditation package.
- Assist in the site surveys.
- Prepare a statement to the DAA about the certification report. The report should include a description of the System and its mission; the results from the testing, document reviews, and hardware and software reviews; remaining system vulnerabilities; and any additional controls or environmental requirements that may be necessary.
- Ensure that the System maintains the system security baseline through audits.
- Notify the System Owner and the DAA (or the DAA's representative) of all configuration changes that may change the System's security baseline.

ATTACHMENT C - SYSTEM ADMINISTRATOR'S SECURITY HANDBOOK